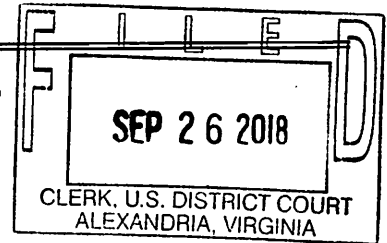


## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

307 YOAKUM PARKWAY, UNIT 714,  
ALEXANDRIA, VIRGINIA 22304

Case No. 1:18-SW-596

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A, incorporated herein by reference

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841(a) and 846	Conspiracy to distribute controlled substances
18 U.S.C. § 924(c)	Possession of a firearm in furtherance of a drug trafficking offense

The application is based on these facts:  
See attached affidavit of Task Force Officer Bikeramjit Gill, Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Tobias D. Tobler

Applicant's signature

Bikeramjit Gill, Task Force Officer (ATF)

Printed name and title

Sworn to before me and signed in my presence.

Date: 26 Sep 18

City and state: Alexandria, Virginia

/s/

Ivan D. Davis

United States Magistrate Judge

ATTACHMENT A

*Property to be Searched and Seized*

The property to be searched is known as 307 Yoakum Parkway, Unit 714, Alexandria, Virginia 22304 (the “Premises”). The Premises are a one-story apartment unit on the seventh floor of an apartment building. The numeric “307” is displayed on top of the front door of the apartment complex. The numeric “714” is located in the center of the light green door to the Premises, attached to a silver door bell. The Premises door has a silver door knob on the right side with two dead bolt locks above it.

The property to be seized from the Premises is an Apple iPhone in a purple case (the “Device”). This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

*Records to be Seized*

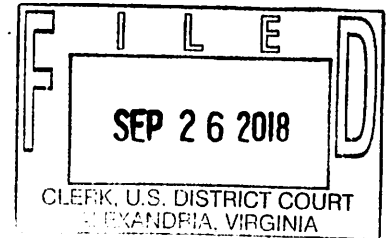
1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1) and 846 and/or 18 U.S.C. § 924(c) and involve OZAN PIROGLU, including:

- a. Any records relating to the obtaining, secreting, transfer, concealment, possession and storage of controlled substances and/or firearms, including documents, notes, ledgers, receipts, bank statements, money drafts, letters of credit, money orders, cashier's checks, pass books, and bank checks;
- b. Any communications relating to the obtaining, secreting, transfer, concealment, possession and storage of controlled substances and/or firearms, including voice messages, text messages, and messages sent through electronic communication applications;
- c. Any records reflecting names, addresses, and telephone numbers of the individuals with whom PIROGLU may have had contact;
- d. Photographs of controlled substances, controlled substances paraphernalia, firearms, ammunition, and firearm accessories, including photographs of PIROGLU and/or other individuals in possession of these items, and photographs showing the associations of these individuals;
- e. Any information recording PIROGLU's schedule or travel from August 21, 2018 to the present;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

IN THE UNITED STATES DISTRICT COURT FOR  
THE EASTERN DISTRICT OF VIRGINIA



IN THE MATTER OF THE SEARCH OF  
307 YOAKUM PARKWAY, UNIT 714,  
ALEXANDRIA, VIRGINIA 22304

No. 1:18-SW-596

AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Bikeramjit Gill, being duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I have been an Alexandria Police Department ("APD") Detective since September 2006. Since January 2014, I have served in the Violent Crimes Section, investigating various violent criminal offenses, including homicide. I am also currently a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") Northern Virginia Violent Crimes Task Force. In this capacity, I investigate individuals involved in the illegal possession and transfer of firearms, violent crimes involving firearms, and narcotics trafficking. As part of these investigations, I have analyzed phone and internet records, and participated in the search and seizure of electronic devices, including cellular phones and "smart" phones.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 307 Yoakum Parkway, Unit 714, Alexandria, Virginia 22304 (the "Premises"), further described in Attachment A, and to authorize the seizure and examination of property—an Apple iPhone in a purple case (the "Device")—believed to be located at the Premises, and to extract from that property electronically stored information described in Attachment B.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### PROBABLE CAUSE

4. On or about August 15, 2018, Alexandria Police Department (“APD”) officers responded to a report of a robbery at 307 Yoakum Parkway, Alexandria, Virginia, in the Eastern District of Virginia. At the scene, PIROGLU informed responding officers that two individuals had entered PIROGLU’s apartment and robbed PIROGLU at gun point. Officers thereafter accompanied PIROGLU to the Premises—a unit in a nearby apartment complex.

5. Once in the Premises, officers detected the strong odor of marijuana, and observed suspected marijuana residue in a plastic bag. PIROGLU advised law enforcement that the robbers had stolen \$5000 in cash, a laptop computer, and PIROGLU’s two guns—a shotgun and a handgun. However, during a security sweep of the Premises, officers found a shotgun hidden in a pair of pants.

6. When confronted by officers with inconsistencies in his account, PIROGLU admitted that the robbers had come to the Premises to purchase marijuana from PIROGLU. Once in the apartment, the robbers drew a firearm on PIROGLU, and robbed him of the marijuana, a handgun, cash, and other valuables. PIROGLU later reported to investigators that, following the robbery, he had to keep his shotgun by the Premises door for protection.

7. On or about August 21, 2018, investigators obtained and executed a warrant authorizing a search of the Premises. During the search, law enforcement located PIROGLU’s suspected belongings in the dining room. In one corner of the dining room, investigators recovered, among other things, mail matter and court documents addressed to PIROGLU at the Premises.

8. In an adjacent corner of the dining room, investigators found a navy blue bag containing five separate packages of a substance that field-tested positive for marijuana. The marijuana weighed a total of 68.55 grams, including packaging. Based upon my training, experience, and knowledge of this case, I believe that the amount and manner in which the marijuana was packaged is consistent with distribution. In the same corner of the dining room, law enforcement found a Mossberg 88 20 gauge shotgun bearing serial number MV72607R and a bag containing ammunition. In the living room, investigators found PIROGLU's driver's license and multiple credit cards, as well as an iPhone.

9. Following the search of the Premises, law enforcement searched the iPhone, which investigators suspected belonged to PIROGLU. The search revealed numerous photographs of PIROGLU, as well as suspected marijuana in distribution quantities packaged for distribution. The search also revealed extensive text messages between the Device user—identified on the Device as “Ozan”—and other individuals in which “Ozan” coordinated the sale and delivery of controlled substances, including marijuana.

10. On or about September 21, 2018, the Honorable Theresa Carroll Buchanan, United States Magistrate Judge, Eastern District of Virginia, issued a complaint and arrest warrant for PIROGLU, charging that, on or about August 21, 2018, PIROGLU possessed with the intent to distribute a mixture and substance containing a detectable amount of marijuana, a Schedule I controlled substance, in violation of Title 21, United States Code, Section 841(a)(1), and possessed a firearm in furtherance thereof, that is, a Mossberg 88 20 gauge shotgun, in violation of Title 18, United States Code, Section 924(c)(1)(A).

11. On or about September 25, 2018, investigators went to the Premises to arrest PIROGLU. When law enforcement encountered PIROGLU at the Premises doorway,

PIROGLU was holding in his hand an Apple iPhone with a purple case (the “Device”). An investigator removed the Device from PIROGLU’s hand, and placed it on top of a crate inside the Premises doorway. Investigators did not seize the Device at that time.

12. From my training and experience—including my experience in this case—I know that individuals who deal in illegal controlled substances and/or firearms, and/or who possess firearms in furtherance of such illegal activity, commonly maintain on their personal electronic devices (including cellular telephones) electronic and photographic records relating to the obtaining, secreting, transfer, concealment, possession, and storage of drugs and/or firearms, including: documents, notes, ledgers, receipts, bank statements, money drafts, letters of credit, money orders, cashier’s checks, pass books, and bank checks.

13. From my training and experience—including my experience in this case—I know that individuals who deal in illegal controlled substances and/or firearms, and/or who possess firearms in furtherance of such illegal activity, commonly maintain on their personal electronic devices (including cellular telephones) communications and records of communications relating to the obtaining, secreting, transfer, concealment, possession, and storage of drugs and/or firearms, including voice messages, text messages, and messages sent through electronic communications applications.

14. From my training and experience—including my experience in this case—I know that individuals who deal in illegal controlled substances and/or firearms, and/or who possess firearms in furtherance of such illegal activity, commonly maintain on their personal electronic devices (including cellular telephones) records that reflect the names, addresses, and telephone numbers of the individuals with whom they conduct such transactions.



15. From my training and experience—including my experience in this case—I know that individuals who deal in illegal controlled substances and/or firearms, and/or who possess firearms in furtherance of such illegal activity, commonly maintain on their personal electronic devices (including cellular telephones) photographs of drugs, drug paraphernalia, firearms, ammunition, and firearm accessories, as well as photographs of individuals (including the device user and associates) in possession of these items.

#### TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another

location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

21. *Manner of execution.* Because the forensic examination of the Device would occur only after the Device is in law enforcement's possession, the examination would not involve physical intrusion onto a premises. Consequently, I request that the Court authorize execution of the this forensic examination at any time in the day or night.

CONCLUSION


22. I submit that this affidavit supports probable cause for a warrant authorizing the search of the Premises, described in Attachment A, to seek the items described in Attachment B.

Respectfully submitted,



Task Force Officer Bikeramjit Gill, ATF

Subscribed and sworn to before me  
On this 26<sup>th</sup> day of September, 2018:



/s/

Ivan D. Davis

United States Magistrate Judge

ATTACHMENT A

*Property to be Searched and Seized*

The property to be searched is known as 307 Yoakum Parkway, Unit 714, Alexandria, Virginia 22304 (the “Premises”). The Premises are a one-story apartment unit on the seventh floor of an apartment building. The numeric “307” is displayed on top of the front door of the apartment complex. The numeric “714” is located in the center of the light green door to the Premises, attached to a silver door bell. The Premises door has a silver door knob on the right side with two dead bolt locks above it.

The property to be seized from the Premises is an Apple iPhone in a purple case (the “Device”). This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

*Records to be Seized*

1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1) and 846 and/or 18 U.S.C. § 924(c) and involve OZAN PIROGLU, including:

- a. Any records relating to the obtaining, secreting, transfer, concealment, possession and storage of controlled substances and/or firearms, including documents, notes, ledgers, receipts, bank statements, money drafts, letters of credit, money orders, cashier's checks, pass books, and bank checks;
- b. Any communications relating to the obtaining, secreting, transfer, concealment, possession and storage of controlled substances and/or firearms, including voice messages, text messages, and messages sent through electronic communication applications;
- c. Any records reflecting names, addresses, and telephone numbers of the individuals with whom PIROGLU may have had contact;
- d. Photographs of controlled substances, controlled substances paraphernalia, firearms, ammunition, and firearm accessories, including photographs of PIROGLU and/or other individuals in possession of these items, and photographs showing the associations of these individuals;
- e. Any information recording PIROGLU's schedule or travel from August 21, 2018 to the present;



2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.